U.S. Department of Transportation
United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
(703)-267-2996

COMDTINST 5230.50
2 MAR 1993

COMMANDANT INSTRUCTION 5230.50

Subj: Remote Access Software (RAS) Use and Security Procedures

Ref: (a) Automated Information System (AIS) Security Manual, COMDTINST M5500.13A
(b) Standard Workstation Security Handbook, COMDTINST M5500.17

1. PURPOSE. This instruction prescribes the use of Remote Access Software (RAS) and establishes procedures and controls to limit automated information security risks. The intended users are Regional System Managers, System Operators, and District/MLC IRM staffs.

2. DISCUSSION.

   a. Remote Access Software (RAS) is a system of software products which enhances support of the Coast Guard Standard Workstation (CGSW). RAS enable authorized personnel to provide remote support for the BTOS/CTOS environment.

   b. All systems subject to access by RAS must have Unisys' proprietary BNET II software installed. BNET II provides the underlying network protocols necessary for RAS operation over the CGDN, Local Area Networks (LAN), or via modem.

2 c RAS is comprised of two pieces of software, Mirror Image and Hotline. User documentation is included for each component of the software.

(1) Mirror Image enables a system to become a source cluster. These are systems used by Regional System Managers (RSM) to remotely monitor or control a target cluster.

(2) Hotline enables a system to become a target cluster. Systems subject to access by RAS must have Hotline. installed. Once installed, these systems cannot monitor or control a source cluster.

3. PROCEDURES.

a. RSMs will coordinate installation and configuration of the appropriate RAS components for all units in their area of responsibility. RSMs or appropriate members of cognizant DT/t/IRM staff will ensure the local system operators are versed about security risks and comply with proper security practices and procedures.

b. All incidents of noncompliance with the security procedures and controls described in this instruction shall be reported to the cognizant Automated Data Processing Security Officer (ADPSO) as defined in references (a) and (b). Any successful or attempted incidents of unauthorized access shall also be reported to the cognizant ADPSO. The ADPSO shall forward a copy of the reported incident to Commandant (G-TPS-4).

4. ACTION. Area and District Commanders, Commanders of Maintenance and Logistics commands, Chiefs of Headquarters offices, Commanding Officers/Commanders of Headquarters units, unit Commanding Officers, Commander Activities Europe, and unit Officers in Charge shall ensure compliance with this Instruction.

D.E. CIANCATLINI
Chief, Office of Command,
Control and Communications

Encl: (1) Security Risks and Procedures for RAS

SECURITY RISKS AND PROCEDURES FOR RAS

POTENTIAL SECURITY RISKS. When BNET II and RAS are loaded, there is an increased risk of unauthorized access over the Coast Guard Data Network (CGDN).

1. This occurs when BNET II is installed on two or more nodes and they are configured to connect. Functions such as viewing files and copying files may be available to anyone on the network depending on the Remote System's passwords. For places that have a LAN, this ability and risk exist today and will increase as additional nodes on the CGDN gain this ability. In addition, as the number of people who have access to a CGSW with BNET II loaded and configured increases, the risk of unauthorized access and disclosure of information also increases.

2. Once the network is established, RAS can function. The source site can remotely control the target terminal.

SECURITY PROCEDURES FOR RAS.

1. AIS Security. Automated Information System (AIS) Security procedures as prescribed in references (a) and (b) must be followed.

    a. Proper passwording schemes shall be followed as outlined in reference (a), paragraph 17.C. RAS can not bypass passwords. If the source site operator does NOT know the proper passwords, there is less risk of unauthorized access.

    b. System Operators and System Managers shall implement limited command sets. The HOTLINE command installs the BENT II and RAS services at target sites. When RAS is loaded, this command is put into sys.cmds file and RAS.cmds file. Only the system administrator or other command-designated person (e.g. one person in each duty section) shall have access to these command sets.

2. Software Configuration. To limit unwanted access to any system with RAS installed, configure BNET II to limit the number of systems to which a source or target can connect.

    a. Both the source and target sites must be configured to establish a connection. More specifically, the source must have the target's BNET II node name and BNET II node address in its node table, and the target must have the source's node name and BNET II node address in its node table. This establishes a directory of accessible

systems. Entries in the node table shall be kept to minimum.

(1) For example, a small boat station would only enter the source system of the RSM that supports it. The RSM source node would only have the 12-15 nodes for which the RSM provides support and the district node from which the RSM receives support.

(2) The node at the district or MLC that provides support would have the RSM nodes entered.

(3) Other nodes may be entered then removed on an as needed basis. For example, if there is an on-going problem at a unit that cannot be corrected by the RSM, the RSM may remotely configure the unit for access by the District IRM staff or other authorized CG support organization. Once the problem is resolved, the RSM would reconfigure the unit's node table to the original limited state.

b. Another security control implemented by software configuration is the ability to limit the number of X.25 virtual circuits available when the BNET II X.25 media service is installed. This prevents an unauthorized person from having access to another node during a legitimate RAS session. Limiting the number of virtual circuits does not affect the number of virtual circuits available to electronic mail.

(1) At target sites, this number is set by the automated installation routine and shall not be changed.

(2) At source sites, this number may be increased, but shall be limited to the number of concurrent RAS sessions from the support node (plus one for diagnostics). This may be needed if two sites are being assisted simultaneously from workstations on the same support node.

c. All RAS sessions shall be conducted in the foreground and monitored by the local system administrator. The feature that allows an RSM to work in the background while the local user works on the terminal shall NOT be enabled.

3. Installation Procedures.

a. BNET II software and RAS software shall not be loaded, booted, or run on SSAMPS or Secure SSAMPS systems.

b. RAS source software shall only be used at RSM, IRM, program manager, and Headquarters units support

clusters. It shall not be loaded at other sites from which support is not normally provided (e.g. small boat stations, MSOs with no RSM, etc.) This limits the number of sites which have the ability to remotely control other clusters. When support personnel travel, they may bring the source software for emergency support, but it shall be run from the floppy, not loaded onto the local hard disk. Source software shall not be left at that unit.

c. For sites connected to the CGDN, an automated routine for all needed BNET II services and RAS is provided with the installation package.

(1) This routine is run from a floppy disk and installs the needed services into memory. The floppy disk and associated files shall NOT be loaded on or run from a hard disk. The BNET II services and RAS shall NOT be automatically installed at system initialization. The floppy shall be available only to command-designated personnel (e.g. system manager, one person per duty section).

(2) Target site system services must be de-installed after each active RAS session by the support site. This can be accomplished by remote booting the target site before terminating the session.

d. Source sites shall also de-install the BNET II X.25 service when not in an active RAS session using the Net Control Center facility. This stops access from the nodes over the X.25 wide area network and limits the scope of access to the systems. Support sites shall NOT install the RAS target software into memory. This will prohibit another node from taking remote control of their system.